

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
22 June 2006 (22.06.2006)

PCT

(10) International Publication Number
WO 2006/065002 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/KR2005/000490

(22) International Filing Date:
24 February 2005 (24.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2004-0108115
17 December 2004 (17.12.2004) KR

(71) Applicant (for all designated States except US): **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161 Gajeong-Dong, Yuseong-Gu, Daejeon 305-350 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KIM, Taesung** [KR/KR]; 114-702 Hanmaeul Apt., Songgang-Dong, 200-4, Yuseong-Gu, Daejeon 305-756 (KR). **JIN, Seung Hun** [KR/KR]; 104-1405 Baekhap Apt., Wolpyeong-Dong, Seo-Gu, Daejeon 302-752 (KR). **CHO, Yeong Sub** [KR/KR]; 107-902 Hanaro Apt., Wolpyeong-Dong, Seo-Gu, Daejeon 302-748 (KR). **CHO, Sang Rae** [KR/KR]; 103-1505 Jindalrae Apt., Wolpyeong-Dong, Seo-Gu, Daejeon 302-754 (KR). **CHOI,**

Dae Seon [KR/KR]; 101-508 Hwangsil Town Apt., Wolpyeong-Dong, Seo-Gu, Daejeon 302-792 (KR). **NOH, Jong Hyouk** [KR/KR]; B-401 TwinVilla Jangdae-Dong 306-10, Yuseong-Gu, Daejeon 305-308 (KR). **KIM, Seung Hyun** [KR/KR]; 105-804 Garammaeul Apt., Dowon-Dong, 1439 Dalseo-Gu, Daegu 704-791 (KR).

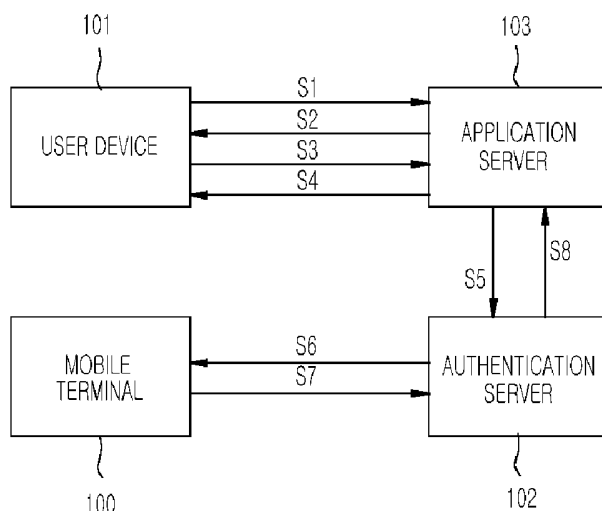
(74) Agent: **LEE, Hwa Ik**; Young International Patent & Law Firm, 4th Fl. Yosam Bldg. 648-23, Yoksam-Dong, Kangnam-Gu, Seoul 135-748 (KR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: USER AUTHENTICATION METHOD IN ANOTHER NETWORK USING DIGITAL SIGNATURE MADE BY MOBILE TERMINAL



(57) Abstract: Disclosed is a user authentication method in another network using a digital signature made by a mobile terminal that includes the steps of a user device connecting to an application server by transmitting an ID to the application server, the application server generating and transmitting random data corresponding to the ID to the user device and transmitting the generated random data and the ID transmitted from the user device to an authentication server, the authentication server transmitting the random data to the corresponding mobile terminal, and the mobile terminal making the digital signature with respect to the random data using a private key of a certificate and transferring the digital signature to the application server. The application server can authenticate the user stronger than the password type authentication method, and the user can use the digital signature for the

authentication without installing a certificate in a user device such as a PC, a notebook computer, a PDA, etc., so that the convenience and the security can be increased.



Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Description

USER AUTHENTICATION METHOD IN ANOTHER NETWORK USING DIGITAL SIGNATURE MADE BY MOBILE TERMINAL

Technical Field

- [1] The present invention relates to a user authentication method in another network using a digital signature made by a mobile terminal, and more particularly to a user authentication method in another network using a digital signature made by a mobile terminal that enables an application server of a wire/wireless Internet to exploit the mobile terminal owned by a user when the application server authenticates the user.

Background Art

- [2] The authentication is a procedure of judging whether a person or an object is surely the actual reported person or object. The authentication in a public network including an individual network or Internet is mostly performed through the use of a password when a login is made. A person who knows the password is once considered to be a believable user. All the users first register their desired passwords, and thereafter, they should remember and use the previously reported passwords whenever the authentication procedure is required.
- [3] The mobile terminal has a built-in key code, and a device authentication of the terminal may be performed in a mobile network. Recently, a certificate may be built in a smart card such as a USIM (Universal Subscriber Identity Module) in order to perform an authentication usable in financial transaction and so on.
- [4] The mobile terminal has become a universal device that a modern possesses for making a phone call all the time or almost every day. The advantages of the mobile terminal having a built-in smart card as an authentication device are that the mobile terminal uses a certificate that is an authentication method stronger than the existing password-based authentication and or it is not necessary to possess a separate device such as a smart card for the authentication.
- [5] In an electronic transaction that requires a high-level stability such as Internet banking, the authentication is performed using a certificate stronger than the conventional password-based authentication.
- [6] However, a public PC in a place such as a government office, a library, a PC game room, etc., is not safe enough to store a certificate and private key. Accordingly, before performing the Internet banking, the user should perform a procedure of installing a certificate in the public PC and then delete it after he/she uses it, and this causes the user inconvenience. Additionally, the certificate should separately be kept in a device that has an excellent security such as a smart card rather than be stored in a personal

PC, a notebook computer, a PDA, etc., and this also causes inconvenience.

Disclosure of Invention

Technical Problem

[7] Therefore, the present invention has been made to solve the above-mentioned problems occurring in the prior art, and an object of the present invention is to provide a user authentication method in another network using a digital signature made by a mobile terminal that enables an application server to perform a user authentication using the digital signature made by the mobile terminal of the user when the user connects to the application server through a PC, a notebook computer, a PDA, etc., for a safer and stronger authentication of the application server.

[8] Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention.

Technical Solution

[9] In order to accomplish the above-mentioned objects, a user authentication method in another network using a digital signature made by a mobile terminal according to the present invention comprises the steps of a) a user device connecting to an application server by transmitting an ID to the application server, b) the application server generating and transmitting random data corresponding to the ID to the user device and transmitting the generated random data and the ID transmitted from the user device to an authentication server, c) the authentication server transmitting the random data to the corresponding mobile terminal, and d) the mobile terminal making the digital signature with respect to the random data using a private key of a certificate and transferring the digital signature to the application server.

[10] The step c) may further comprise the step of the authentication server searching the mobile terminal of the user that corresponds to the ID.

[11] Additionally, the step d) comprises the steps of outputting the random data to the mobile terminal, the mobile terminal making the digital signature using the private key of the certificate, the mobile terminal transmitting the digital signature to the authentication server, the authentication server verifying the digital signature and transmitting a result of authentication to the application server, and the application server deciding whether to permit an access of the user device in accordance with the result of authentication.

[12] It is preferable that the step d) compares the random data between the user device and the mobile terminal through by the steps of the user device and the mobile terminal hashing the random data using a hash function that is one-way function, dividing a

hash value into a predetermined number of fragments and giving numbers to the respective fragments, and displaying the fragment of the hash value that corresponds to a certain input number among the given numbers on the user device and the mobile terminal.

Advantageous Effects

- [13] According to the user authentication method in another network using a digital signature made by a mobile terminal according to the present invention, if the user device of another network is authenticated using the digital signature made by the mobile terminal, the application server can authenticate the user stronger than the password type authentication method. Additionally, it is not required for the user to possess a separate authentication or to install the note of authentication in many user devices, and thus the convenience and the security can be increased.

Brief Description of the Drawings

- [14] The above objects, other features and advantages of the present invention will become more apparent by describing the preferred embodiments thereof with reference to the accompanying drawings, in which:
- [15] FIG. 1 is a view illustrating the whole construction of a system and an authentication procedure according to an embodiment of the present invention; and
- [16] FIG. 2 is a flowchart illustrating a procedure of comparing random data between a user device and a mobile terminal according to an embodiment of the present invention.

Best Mode for Carrying Out the Invention

- [17] Now, a user authentication method in another network using a digital signature made by a mobile terminal according to a preferred embodiment of the present invention will be described in detail with reference to the annexed drawings.
- [18] FIG. 1 is a view illustrating the whole construction of a system and an authentication procedure according to an embodiment of the present invention which enables a user who possesses a mobile terminal to connect to a wire Internet or a wireless Internet with an Internet-connectable device such as a computer, a notebook computer, a PDA, etc., through an authentication procedure performed by an authentication server of a mobile communication network.
- [19] Referring to FIG. 1, the system according to the present invention includes a mobile terminal 100, a user device 101, an authentication server 102 and an application server 103.
- [20] The mobile terminal 100 owned by a user has a digital authentication function.
- [21] The user device 101 is a kind of an Internet-connectable device such as a PC, a notebook computer, a PDA, etc., and a device that a user can access, use and carry.

- [22] The authentication server 102 can directly communicate with the user's mobile terminal 100, and stores a terminal number for the user's ID.
- [23] The application server 103, which is a server that needs to authenticate the user device, is communicable with servers of sites of Internet shopping malls, the electronic government, banks, companies, etc., and the authentication server of the mobile communication network.
- [24] In the system as constructed above, the user accesses the application server 103 through the user device 101 (step S1), and in this case, the application server 103 requests the user to input the user's ID (step S2). If the user inputs the ID (step S3), the application server 103 generates and transmits random data to the user device 101 (step S4), and simultaneously transmits the random data and the user's ID to the authentication server (step S5).
- [25] Then, the authentication server 102 searches for the user's mobile terminal 100 corresponding to the ID and transmits the random data to the mobile terminal 100 (step S6). The user confirms whether the random data from the user device 101 coincides with that from the mobile terminal 100, and if they coincide with each other, the user makes a digital signature with a private key of the certificate with respect to the random data.
- [26] The mobile terminal 100 transmits the digital signature to the authentication server (step S7), and the authentication server 102 verify the digital signature and then transmits the result of authentication to the application server 103 (step S8). The application server permits the access of the user device according to the result of authentication.
- [27] FIG. 2 is a flowchart illustrating the procedure of comparing the random data between the user device and the mobile terminal according to an embodiment of the present invention. Specifically, FIG. 2 shows the logic for enabling the user to easily compare the random data between the user device 101 and the mobile terminal 100.
- [28] Referring to FIG. 2, since the typical random data subject to be a large size, it is not easy for the user to compare them with his/her eyes. The user device 101 and the mobile terminal 100 hash the random data using a hash function that is a one-way function (step S20), divide the hash value into 10 units, i.e., segments, and give numbers 0 to 9 to the respective segments (step S21). If the user inputs a certain figure, the devices display the fragment of the hash value corresponding to the input number on a display screen (step S22). Accordingly, the user can easily compare the random data (step S23).
- [29] The logic for the user's easy comparing of the random data between the user device 101 and the mobile terminal 100 as illustrated in FIG. 1 can be implemented by a program and stored in a computer-readable recording medium (such as a CD ROM,

RAM, ROM, floppy disc, hard disc, optomagnetic disc, etc.). This process can be easily performed by an ordinary skilled in the art that the present invention belongs to, and thus the detailed explanation thereof will be omitted.

[30]

Industrial Applicability

[31] As apparent from the above description, according to the user authentication method in another network using a digital signature made by a mobile terminal according to the present invention, if the user device of another network is authenticated using the digital signature made by the mobile terminal, the application server can authenticate the user stronger than the password type authentication method. Additionally, it is not required for the user to possess a separate authentication or to install the certificate in many user devices, and thus the convenience and the security can be increased.

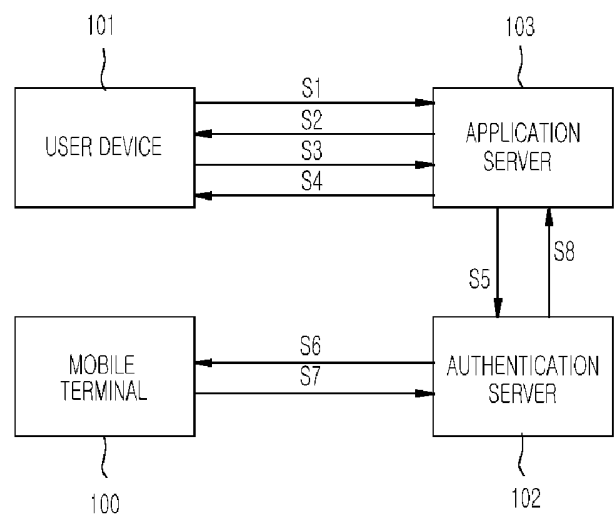
[32] The forgoing embodiments are merely exemplary and are not to be construed as limiting the present invention. The present teachings can be readily applied to other types of apparatuses. The description of the present invention is intended to be illustrative, and not to limit the scope of the claims. Many alternatives, modifications, and variations will be apparent to those skilled in the art.

[33]

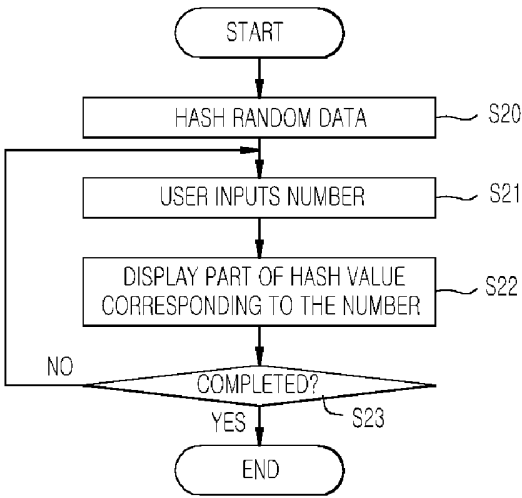
Claims

- [1] A user authentication method in another network using a digital signature made by a mobile terminal, comprising the steps of:
- a) a user device connecting to an application server by transmitting an ID to the application server;
 - b) the application server generating and transmitting random data corresponding to the ID to the user device and transmitting the generated random data and the ID transmitted from the user device to an authentication server;
 - c) the authentication server transmitting the random data to the corresponding mobile terminal; and
 - d) the mobile terminal making the digital signature with respect to the random data using a private key of a certificate and transferring the digital signature to the application server.
- [2] The user authentication method as claimed in claim 1, wherein the step c) further comprises the step of the authentication server searching the mobile terminal of the user that corresponds to the ID.
- [3] The user authentication method as claimed in claim 1, wherein the step d) comprises the steps of:
- outputting the random data to the mobile terminal;
 - the mobile terminal making the digital signature using the private key of the certificate;
 - the mobile terminal transmitting the digital signature to the authentication server;
 - the authentication server verifying the digital signature and transmitting a result of authentication to the application server; and
 - the application server deciding whether to permit an access of the user device in accordance with the result of authentication.
- [4] The user authentication method as claimed in claim 1, wherein the step d) compares the random data between the user device and the mobile terminal through the steps of:
- the user device and the mobile terminal hashing the random data using a hash function that is a one-way function;
 - dividing a hash value into a predetermined number of fragments and giving numbers to the respective fragments; and
 - displaying the fragment of the hash value that corresponds to a certain input number among the given numbers on the user device and the mobile terminal.

[Fig. 1]



[Fig. 2]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2005/000490

A. CLASSIFICATION OF SUBJECT MATTER IPC7 H04L 9/32 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC7 H04L Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched KR : AS ABOVE Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 02/15626 A1 (Telefonaktiebolaget LM Ericsson) 21 Feb 2002 (see abstract, figure 1,2,3, pages 7~8, claim 22)	1 ~ 3 4
A	WO 2004/056038 A1 (Nokia Corporation) 1 July 2004 (see abstract)	1 ~ 4
A	EP 1487176 A1 (Lucent Technologies Inc) 15 Dec 2004 (see abstract)	1 ~ 4
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 14 SEPTEMBER 2005 (14.09.2005)		Date of mailing of the international search report 16 SEPTEMBER 2005 (16.09.2005)
Name and mailing address of the ISA/KR  Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140		Authorized officer LEE, Dong Hwan Telephone No. 82-42-481-5755 

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2005/000490

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
AU200183949A1	25.02.2002	AU200183949A5	25.02.2002
		EP01323323A1	02.07.2003
		EP1323323A1	02.07.2003
		GB200020095A0	04.10.2000
		GB2366139A	27.02.2002
		GB2366139A1	27.02.2002
		GB2366139B2	14.07.2004
		US20020034301A1	21.03.2002
		US2002034301AA	21.03.2002
W02004056038A1	01.07.2004	W0200215626A1	21.02.2002
W02004056038A1	01.07.2004	AU2002353354AA	09.07.2004
		W02004056038A1	01.07.2004
EP1487176A1	15.12.2004		
EP1487176A1	15.12.2004	EP01487176A1	15.12.2004
		EP1487176A1	15.12.2004
		JP17004764	06.01.2005
		JP2005004764A2	06.01.2005
		KR1020040105609	16.12.2004
		US20040248554A1	09.12.2004
		US2004248554AA	09.12.2004